SPYWOLF

Security Audit Report

Completed on

May 16, 2023

OVERVIEW

This audit has been prepared for **HAPPY PEPE YACHT CLUB** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

HAPPY PEPE YACHT CLUB

PROJECT DESCRIPTION

According to their whitepaper:

The Happy PEPE Yacht Club (HPYC) is a new project that aims to transform the PEPE the frog meme into a symbol of happiness. The project offers an exclusive collection of NFTs showcasing digital artworks created by talented artists. The HPYC introduces the $HPYC token on the Binance Smart Chain to create an empowering and dynamic ecosystem. The HPYC community embraces joy, creativity, and community to foster limitless potential.

Release Date: Presale starts in May, 2023

Category: Meme token

CONTRACT INFO

Token Name
Happy PEPE Yacht Club

Symbol
HPYC

Contract Address
0x00a628E50412F5f385fDdceF96281e0454438414

Network
Binance Smart Chain

Language
Solidity

Deployment Date
May 09, 2023

Verified?
Yes

Total Supply
420,000,000,000,000

Status
Not launched

TAXES

Buy Tax
9%

Sell Tax
9%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	840000000000000 HPYC
Median Transfer Amount	420000000000000 HPYC
Average Transfer Amount	420000000000000 HPYC
First transfer date	2023-05-09
Last transfer date	2023-05-09
Days token transferred	1

SMART CONTRACT STATS

Calls Count	4
External calls	4
Internal calls	0
Transactions count	4
Uniq Callers	1
Days contract called	1
Last transaction time	2023-05-09 12:17:30 UTC
Created	2023-05-09 12:15:36 UTC
Create TX	0x1f607b92ad18d830e639f0c245b82290910c64656343d1d7d6cff2b6cb6b1110
Creator	0x26d41682b1c2bedb4242dbffe56e16be6cf569c5

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium Risk

Owner can set protections contract once, before trading is enabled.
Owner can set anti bots criteria in the protections contract.
The protections external contract is used to perform checks on regular users with each token buy/sell/transfer.
If protections contract is inappropriate one, unexcluded users from limitations won't be able to buy/sell the token.

The protections contract that perform these checks is not in the scope of the current audit.

```
function setProtectionSettings(bool _antiSnipe, bool _antiBlock) external onlyOwner {
    protections.setProtections(_antiSnipe, _antiBlock);
}

function _transfer(address from, address to, uint256 amount) internal returns (bool) {
..............
return finalizeTransfer(from, to, amount, buy, sell, other);
}

function finalizeTransfer(address from, address to, uint256 amount, bool buy, bool sell, bool other) internal returns (bool) {
if (_hasLimits(from, to)) { bool checked;
    try protections.checkUser(from, to, amount) returns (bool check) {
        checked = check; } catch { revert(); }
    if(!checked) { revert(); }
}
..............
}
```

Informational

Owner can withdraw any tokens from the contract until liquidity is added. Once liquidity is added, the owner can withdraw any tokens from the contract with exception of the native blockchain token (ETH/BNB) and the native contract token (HPYC).

```
function sweepContingency() external onlyOwner {
    require(!_hasLiqBeenAdded, "Cannot call after liquidity.");
    payable(_owner).transfer(address(this).balance);
}

function sweepExternalTokens(address token) external onlyOwner {
    if (_hasLiqBeenAdded) {
        require(token != address(this), "Cannot sweep native tokens.");
    }
    IERC20 TOKEN = IERC20(token);
    TOKEN.transfer(_owner, TOKEN.balanceOf(address(this)));
}
```

Owner can set max wallet limit but cannot set it below 1% of total supply.

```
function setMaxWalletSize(uint256 percent, uint256 divisor) external onlyOwner {
    require((_tTotal * percent) / divisor >= (_tTotal / 100),
    "Max Wallet amt must be above 1% of total supply.");
    _maxWalletSize = (_tTotal * percent) / divisor;
}
```

Owner can set max transaction limit but cannot set it below 0.5% of total supply.

```
function setMaxTxPercent(uint256 percent, uint256 divisor) external onlyOwner {
    require((_tTotal * percent) / divisor >= (_tTotal * 5 / 1000),
    "Max Transaction amt must be above 0.5% of total supply.");
    _maxTxAmount = (_tTotal * percent) / divisor;
}
```

Informational

Owner can exclude address from fees.
Owner can exclude address from transaction limit and wallet limit.
Owner can exclude address from external protection contract's checks.

```
function setExcludedFromFees(address account, bool enabled) public onlyOwner {
    _isExcludedFromFees[account] = enabled;
}

function setExcludedFromLimits(address account, bool enabled) external onlyOwner {
    _isExcludedFromLimits[account] = enabled;
}

function setExcludedFromProtection(address account, bool enabled) external onlyOwner {
    _isExcludedFromProtection[account] = enabled;
}
```

Owner can set buy/sell/transfer fees up to 10%.
Combined buy+sell = 20%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
uint256 constant public maxBuyTaxes = 1000;
uint256 constant public maxSellTaxes = 1000;
uint256 constant public maxTransferTaxes = 1000;
uint256 constant masterTaxDivisor = 10000;

function setTaxes(uint16 buyFee, uint16 sellFee, uint16 transferFee) external onlyOwner {
    require(!taxesAreLocked, "Taxes are locked.");
    require(buyFee <= maxBuyTaxes
            && sellFee <= maxSellTaxes
            && transferFee <= maxTransferTaxes,
            "Cannot exceed maximums.");
    _taxRates.buyFee = buyFee;
    _taxRates.sellFee = sellFee;
    _taxRates.transferFee = transferFee;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

HAPPY PEPE YACHT CLUB

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but can’t lower it than 0.5% of total supply

There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

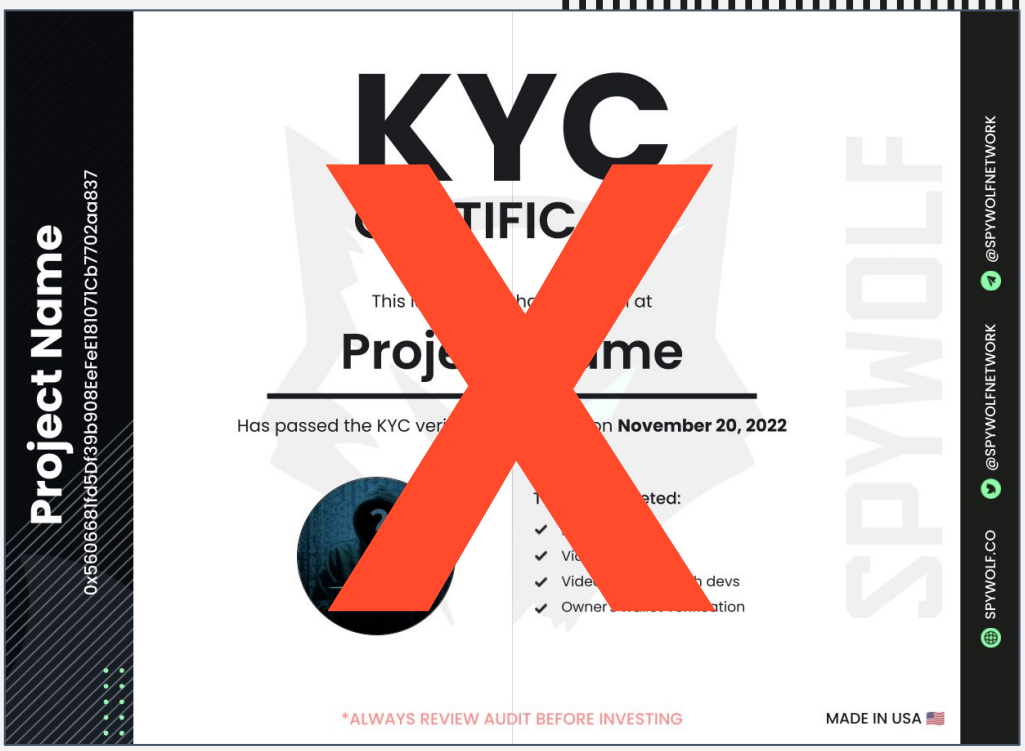
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://happypepeyatch.club/

Domain Registry
https://sav.com

Domain Expiration
2024-05-09

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

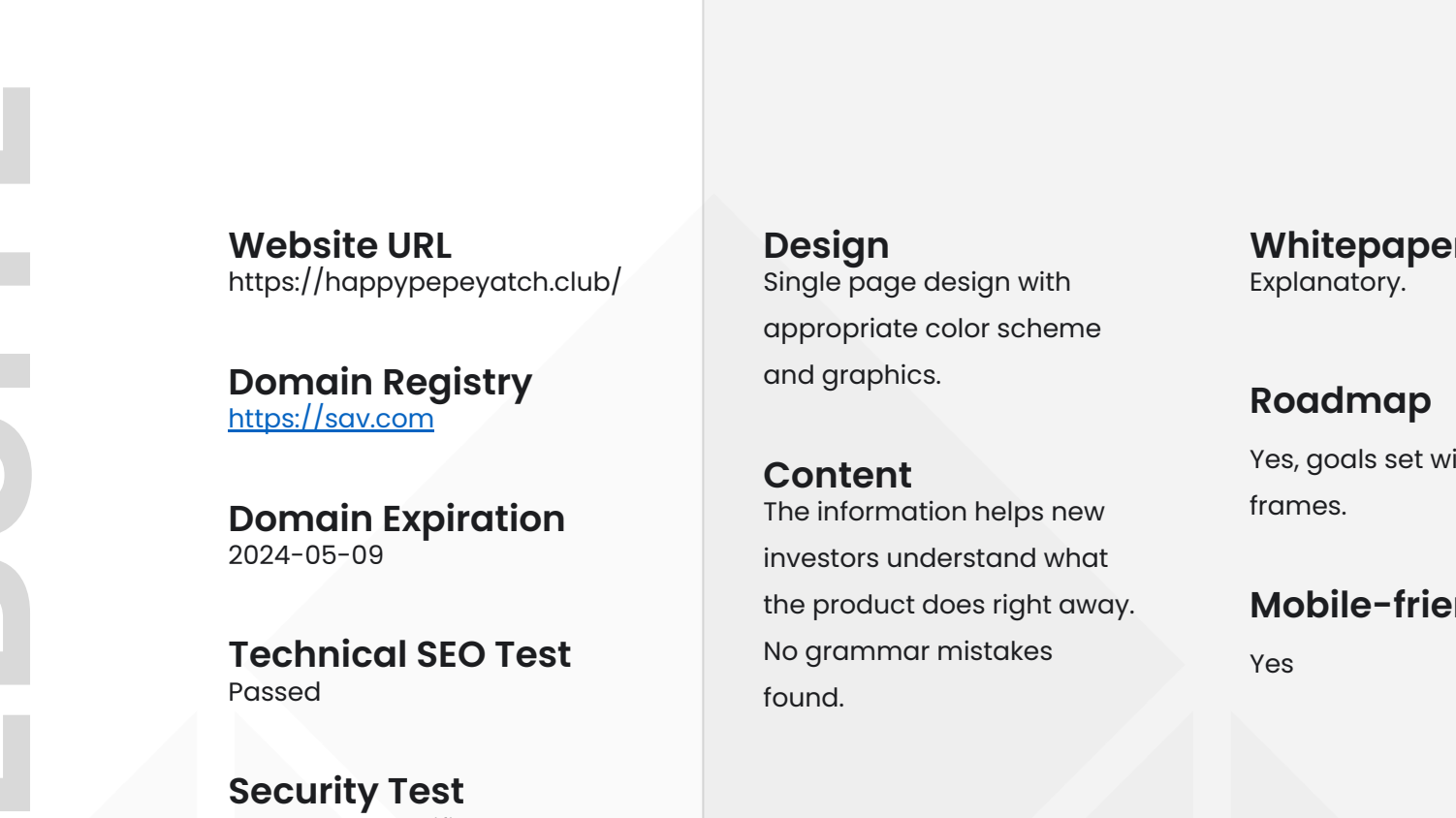
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



happypepeyatch.club

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active.

Twitter

@HappyPEPE_YC

- 8 559 followers
- 2 total posts
- New account

Discord

- Not available

Telegram

@happypepeyatchclub

- 2484 members
- Active mods and members

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.